UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF NEW YORK

MARTINO PIETANZA, BOBBI HODGE, and STEVEN HODGE, on behalf of themselves and all others similarly situated, Plaintiffs, - against - TARGET CORPORATION and JOHN DOES 1-100, Defendant.	Case No. **CLASS ACTION COMPLAINT** **JURY TRIAL DEMANDED**

Plaintiffs Martino Pietanza, Bobbi Hodge, and Steven Hodge ("Plaintiffs") bring this class action complaint on behalf of themselves and all others similarly situated (the "Class"), upon knowledge as to the facts and upon information and belief as to all other matters, based on the investigation of their counsel, Napoli Bern Ripka Shkolnik, LLP, against defendants Target Corporation ("Target"), and John Does 1-100 (collectively, "Defendants") and states as follows:

NATURE OF THE ACTION

1. This is a class action for damages arising from Defendants' failure to secure and to monitor its computer systems to protect Target's customers and the information Target's customers provided to Target in shopping at Target's stores across the United States. More specifically, Target failed to secure and to protect its customers' email addresses, passwords, credit card and debit card numbers, expiration dates, and both mailing and billing addresses, and failed to monitor its systems to detect unauthorized foreign software that allowed the theft of its customers' information.

2. On December 19, 2013, Target announced a massive data security breach, of which it had become aware four days earlier on December 15, 2013. During the height of the

holiday shopping season, Target waited four days before announcing to customers and others that the security breach had occurred.

3. As a direct and proximate result of Target's failure to secure its systems and to notify Plaintiffs and all other members of the proposed Class of the theft of their personal and financial information, Plaintiffs, on behalf of themselves and members of the Class, seek actual damages, economic damages, statutory damages, nominal damages, exemplary damages, reasonable attorneys' fees, litigation expenses and the costs of this action.

THE PARTIES

4. Plaintiff Martino Pietanza is a citizen of the State of New York.

5. Plaintiff Bobbi Hodge is a citizen of the State of Illinois.

6. Plaintiff Steven Hodge is a citizen of the State of Illinois.

7. Defendant Target Corporation is a corporation organized and existing under the laws of the state of Minnesota with its headquarters at 1000 Nicollet Mall, Minneapolis, Minnesota 55403. Target is one the largest discount retailers in the United States and conducts its business in all fifty states, including through numerous stores in New York.

8. John Does 1-100 are unknown parties liable for damages caused by the data breach at Target.

JURISDICTION AND VENUE

9. This Court has original jurisdiction pursuant to 28 U.S.C. § 1332(d)(2) because the parties are citizens of different states and the aggregate amount of controversy exceeds the sum or value of $5,000,000, under Class Action Fairness Act, exclusive of interest, and is a class action composed of more than 100 members. There is minimal diversity of citizenship between the proposed class and Target. This Court has supplemental jurisdiction over state law claims

and common law claims pursuant to 28 U.S.C. § 1367(a).

10. This Court also has original jurisdiction pursuant to 28 U.S.C. § 1331 because Plaintiffs' claims under the Federal Stored Communications Act (18 U.S.C. §§ 2701, *et seq*.) arise under the Constitution, laws, or treaties of the United States. Similarly, this Court has supplemental jurisdiction over state law claims and common law claims pursuant to 28 U.S.C. § 1367(a).

11. This Court has personal jurisdiction over Target because Target maintains a regular, systematic, and continuous presence in New York, substantial acts as alleged herein were committed by Target in New York, and Plaintiff and other members of the proposed Class suffered injuries in New York.

12. Venue is proper in this district under 28 U.S.C. § 1391(b)(1), (2), (c) because Target conducts its business in this district, and substantial actions or omissions occurred in this district.

FACTS COMMON TO ALL COUNTS

13. Between November 27, 2013 and December 15, 2013, tens of millions of customers, including Plaintiff and other members of the proposed Class, who shopped at Target stores were subject to the theft of their personal information and their credit card and debit card information. The theft was accomplished by unknown and unauthorized third parties who were able to access such data through software installed on Target's point-of-sales terminals used to swipe magnetic strips on credit and debit cards.

14. The lack of adequate security at Target and on Target's computer systems allowed such third parties to install the software used to accomplish the data breach. Moreover, Target did not adequately monitor its computer systems for the presence of foreign, unauthorized

software, malware, and other rogue programs. Target did not detect the intrusion, which went unnoticed for several weeks during the 2013 holiday shopping season.

15. As a result of the software installed on Target's computer systems, unknown and unauthorized third parties were able to access customer data within Target's computer systems and/or in the course of transmission of the data to various financial institutions.

16. Upon information and belief, Target first discovered this massive data and security breach on December 15, 2013 but did not publicly disclose the breach until four days later on December 19, 2013.

17. More specifically, in relevant part, Target released the following message on its website on December 19, 2013:

> Dear Guest,
>
> We wanted to make you aware of unauthorized access to Target payment card data. The unauthorized access may impact guests who made credit or debit card purchases in our U.S. stores from Nov. 27 to Dec. 15, 2013. Your trust is a top priority for Target, and we deeply regret the inconvenience this may cause. The privacy and protection of our guests' information is a matter we take very seriously and we have worked swiftly to resolve the incident.
>
> We began investigating the incident as soon as we learned of it. We have determined that the information involved in this incident included customer name, credit or debit card number, and the card's expiration date and CVV.
>
> We are partnering with a leading third-party forensics firm to conduct a thorough investigation of the incident and to examine additional measures we can take that would be designed to help prevent incidents of this kind in the future. Additionally, Target alerted authorities and financial institutions immediately after we discovered and confirmed the unauthorized access, and we are putting our full resources behind these efforts.

(*See* https://corporate.target.com/_media/TargetCorp/global/PDF/ImpactedGuestEmail-12-19-updated.pdf) (last visited January 14, 2013).

18. The section of the December 19, 2013 communication titled "FAQs" contained

the following question and answer that demonstrates the widespread nature of the breach and which helps to define the potential Class:

> How do I know if this impacts me?
>
> If you shopped at Target between Nov. 27 and Dec. 15, you should check your account for any suspicious or unusual activity. If you see something that appears fraudulent, REDcard holders should contact Target, others should contact their bank.

19. Although Target claims to have moved swiftly to resolve the incident, Target did not move swiftly in notifying potentially affected customers (or in providing any type of public notice until four days after having discovered the security breach).

20. Despite the substantial threat of identity theft and improper use of customers' financial and personal information – something that is widespread and a continuous concern even without the breach of Target's computer systems – Target failed to notify the public promptly to allow Plaintiffs and the other potential Class members to determine whether their information was a part of the breach and to take measures to protect that information.

21. In fact, upon information and belief, news of the date breach was first published by Brian Krebs, a blogger, at http://krebsonsecurity.com/, on or about December 18, 2013 before Target had notified affected customers.

22. The following day, December 20, 2013, Target released the following information on its website:

> Dear Target Guest,
>
> As you have likely heard by now, Target experienced unauthorized access to payment card data from U.S. Target stores. We take this crime seriously. It was a crime against Target, our team members and most importantly you - our valued guest.
>
> We understand that a situation like this creates stress and anxiety about the safety of your payment card data at Target. Our brand has been built on a 50-year

foundation of trust with our guests, and we want to assure you that the cause of this issue has been addressed and you can shop with confidence at Target.

We want you to know a few important things:

- The unauthorized access took place in U.S. Target stores between Nov. 27 and Dec. 15, 2013. Canadian stores and target.com were not affected.
- Even if you shopped at Target during this time frame, it doesn't mean you are a victim of fraud. In fact, in other similar situations, there are typically low levels of actual fraud.
- There is no indication that PIN numbers have been compromised on affected bank issued PIN debit cards or Target debit cards. Someone cannot visit an ATM with a fraudulent debit card and withdraw cash.
- You will not be responsible for fraudulent charges – either your bank or Target have that responsibility.
- We're working as fast as we can to get you the information you need. Our guests are always the first priority.
- For extra assurance, we will offer free credit monitoring services for everyone impacted. We'll be in touch with you soon on how and where to access the service.

(*See* https://corporate.target.com/_media/TargetCorp/global/PDF/ImpactedGuestEmail-Gregg LetterAndNotification-12-20.pdf) (last visited January 14, 2014).

23. On January 10, 2014, Target confirmed the data breach was far worse than previously believed. In announcing an update on its continuing investigation into the data breach, target revealed that certain customer information – separate from the payment card data previously disclosed – was taken during the breach. Target also disclosed that the number of customers affected by the data breach was substantially higher than initially thought and actually impacted up to 70 million individuals. (*See* http://investors.target.com/phoenix.zhtml?c=65828&p=irol-newsArticle&ID=1889763&highlight=) (last visited January 14, 2014).

24. Then on January 13, 2014, Target posted an additional letter on its website to its

customers:

Dear Target Guests,

As you have probably heard, Target learned in mid-December that criminals forced their way into our systems, gaining access to guest credit and debit card information. As a part of the ongoing forensic investigation, it was determined last week that certain guest information, including names, mailing addresses, phone numbers or email addresses, was also taken.

Our top priority is taking care of you and helping you feel confident about shopping at Target, and it is our responsibility to protect your information when you shop with us.

We didn't live up to that responsibility, and I am truly sorry.

Please know we moved as swiftly as we could to address the problem once it became known, and that we are actively taking steps to respond to your concerns and guard against something like this happening again. Specifically, we have:

1. Closed the access point that the criminals used and removed the malware they left behind.

2. Hired a team of data security experts to investigate how this happened. That effort is ongoing and we are working closely with law enforcement.

3. Communicated that our guests will have zero liability for any fraudulent charges arising from the breach.

4. Offered one year of free credit monitoring and identity theft protection to all Target guests so you can have peace of mind.

In the days ahead, Target will announce a coalition to help educate the public on the dangers of consumer scams. We will also accelerate the conversation–among customers, retailers, the financial community, regulators and others–on adopting newer, more secure technologies that protect consumers.

I know this breach has had a real impact on you, creating a great deal of confusion and frustration. I share those feelings. You expect more from us and deserve better.

We want to earn back your trust and confidence and ensure that we deliver the Target experience you know and love.

We are determined to make things right, and we will.

(*See* https://corporate.target.com/_media/TargetCorp/global/PDF/GreggLetter-ad-version04.pdf) (emphasis added) (last visited January 14, 2014).

25. As Target specifically noted in its disclosure to customers such as Plaintiffs and the other members of the proposed Class, it is Target's "responsibility to protect your information when you shop with us. ***We didn't live up to that responsibility*** . . . ." (*Id.*) (emphasis added).

26. According to the Federal Trade Commission ("FTC"), the range of recognized privacy-related harms are more expansive than economic or physical harm or unwarranted intrusions and that any privacy framework should recognize additional harms that might arise from unanticipated uses of data.

27. Plaintiff Martino Pietanza regularly shops at Target stores, and used his debit card at two of Target's stores in Staten Island, New York several times in the time period between November 27, 2013 and December 15, 2013. At Target's stores, Mr. Pietanza purchased merchandise for his personal and/or family's use.

28. After having used his debit card at Target during the relevant time period, on or about December 20, 2013, Mr. Pietanza tried to use his debit card to make a purchase for food and was told by the merchant that the card was declined. Mr. Pietanza did not understand why his card was declined because there were sufficient funds in his account for the purchase he was trying to make.

29. Mr. Pietanza then called Chase Bank (the issuer of the debit card) and asked why his card had been declined. He was informed by Chase that his card was among those compromised by the data breach at Target and that a freeze had been placed on his debit card. Chase also informed Mr. Pietanza that the freeze had been removed and that he would have no

further problems using his debit card.

30. Several days later, Mr. Pietanza again tried to use his debit card to make a purchase at a CVS store and was again told by the merchant that the card had been declined. Again, Mr. Pietanza called Chase Bank and was again told a freeze had been placed on his card based on the Target data breach.

31. Once again, in or about January 2014, Mr. Pietanza tried to use his debit card to make a purchase for a snow blower and was again told the card had been declined. As he was informed by Chase Bank, a $1,000 per day limit had been placed on his card based on the data breach at Target, which impacted his ability to complete the purchase with his debit card. Finally, Chase Bank sent Mr. Pietanza a new debit card to avoid any further hassle and expense related to the Target data breach.

32. Plaintiffs Bobbi and Steven Hodge shopped at the Target store in Champaign, Illinois during the period November 27, 2013 to December 15, 2013. Mr. and Mrs. Hodge used their debit cards at Target to purchase merchandise for personal and/or family use.

33. Following the data breach at Target, the bank where Mr. and Mrs. Hodge maintain their account linked to their debit cards called them and informed them that their debit cards were on the list of those debit cards affected by the Target data breach. In the days leading up to Christmas, when they needed to use their debit cards for holiday purchases, Mr. and Mrs. Hodge's bank informed them they had suspended charging privileges on their debit cards and that they would be issuing them new cards.

34. When Mr. and Mrs. Hodge received their new cards, they continued to experience difficulty with the new cards and the continued impact from having to deal with the aftermath of the Target data breach.

35. As a direct and/or proximate result of the data breach at Target, Plaintiffs and Class Members have been required to (and will have to continue to) mitigate the actual and potential impact of the data breach at Target on their lives including, among other things, addressing the freezes placed on their debit and credit cards, closing or modifying financial accounts, and closely reviewing and monitoring their credit reports and accounts for unauthorized activity. In addition, Plaintiffs and the Class members have experienced having their cards declined and their transactions impacted based of the effects of the Target data breach. Because Plaintiff's and Class Members' personal information was stolen and compromised, they also now face a significantly heightened risk of identity theft.

CLASS ACTION ALLEGATIONS

36. Plaintiffs bring this action on behalf of themselves and all other persons similarly situated under Rules 23(a) and 23(b)(3) of the Federal Rules of Civil Procedure.

37. The Class is defined to include all persons, according to Target's records, who used credit cards or debit cards at Target Corporation stores throughout the United States and whose personal and/or financial information was breached during the period from on or about November 27, 2013 to on or about December 15, 2013. Excluded from the Class are Target, Target's officers, directors, employees, and subsidiaries, any entity in which Target has a controlling interest, any of Target's affiliates, legal representatives, attorneys, heirs, and assigns, government entities or agencies, and any judicial officer presiding over this matter and the members of their immediate families and judicial staff.

38. This action satisfies the numerosity, predominance, typicality, adequacy, and/or superiority requirements of Rule 23 of the Federal Rules of Civil Procedure.

39. Plaintiffs are members of the Class they seek to represent.

40. Plaintiffs do not know the exact size of the class. Such information is in Target's possession due to the nature of the trade and business involved.

41. There are numerous common questions of law and fact as to Plaintiffs and the other all members of the Class, which predominate over any questions affecting individual members of the Class, including but not limited to:

a. Whether Target unlawfully maintained, lost, or disclosed personal and/or financial information of the members of the Class;

b. Whether Target failed to protect its customers' personal information with industry-standard protocols and technology;

c. Whether Defendants failed to use reasonable care and commercially reasonable methods to secure and safeguard its customers' sensitive personal and financial information;

d. Whether Target properly implemented security measures to protect customers' personal and financial information from unauthorized capture, dissemination, and misuse;

e. Whether Target failed to maintain and implement reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the data breach;

f. Whether Target failed to monitor its computer systems for unauthorized software, malware, and other rogue programs that allowed third parties to access customers' personal and financial information;

g. Whether Target failed to disclose material facts relating to the character and quality of its data security practices;

h. Whether Target knew that is representations about its security practices were false and misleading and continued to disseminate them;

i. Whether Target took reasonable measures to determine the extent of the security breach after it was first discovered;

j. Whether Target unreasonably delayed in notifying Plaintiffs and affected customers of the data breach;

k. Whether Target's method of informing customers of the security breach and its description of the breach and potential exposure to damages as a result of

the breach was unreasonable;

l. Whether Target's conduct was negligent and/or grossly negligent;

m. Whether Target's conduct violated the Stored Communications Act (18 U.S.C. § 2702);

n. Whether Target's conduct violated New York General Business Law § 349;

o. Whether Target's conduct violated New York General Business Law § 899-aa;

p. Whether Target's conduct violated the Illinois Consumer Fraud and Deceptive Business Practices Act (815 I.L.C.S. 505/1, *et seq.*); and

q. Whether Target's conduct violated the Illinois Personal Information Protection Act (815 I.L.C.S. 530/1, *et seq.*);

42. Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs and the other Class members were harmed in the same way and suffered the same theft of their personal and financial information during the data breach of Target's computer systems.

43. Plaintiffs will fairly and adequately protect the interests of the Class, and Plaintiffs have hired counsel able and experienced in prosecuting this action. Plaintiffs have no claims antagonistic to those of the Class.

44. The members of the Class are ascertainable from Target's records maintained in its databases. This information is the same information Target used to notify banks and other financial institutions about the data breach concerning the particular credit card and debit card information that was stolen.

45. A class action is superior to other available methods for the full and efficient adjudication of the controversy. The Court and the parties would benefit from the economies in litigating common issues on a class-wide basis instead of a repetitive individual basis. The size of each putative Class member's damages is too small to make individual litigation an

economically viable option.

46. Plaintiffs anticipate no unusual difficulties in the management of the Class.

47. Plaintiffs' and the Class members' damages include, but are not limited to:

a. direct financial expenses due to unauthorized use of credit card account information;

b. the hassle and expense of securing replacement of compromised credit card and debit card numbers, passwords, and employment of monitoring services to protect against fraud;

c. the deprivation of opportunities to safeguard personal and financial information, monitor credit card activity, and take steps to prevent identity theft;

d. losses as a result of computer viruses targeting corporations, individuals, and other entities using email addresses and personal information obtained; and

e. potential disclosure of private email communications.

48. Target is liable to Plaintiffs and the Class for monetary, statutory, equitable, and consequential damages based on the foregoing acts, together with Plaintiffs' reasonable attorney's fees and costs this action.

AS AND FOR A FIRST CAUSE OF ACTION
(Violation of the Federal Stored Communications Act, 18 U.S.C. § 2702)

49. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

50. The Stored Communications Act ("SCA") provides consumers with redress if a company mishandles their electronically stored information. The SCA was designed, in relevant part, to protect individuals' privacy interests in personal and proprietary information.

51. Section 2702(a)(2)(A) of the SCA provides "a person or entity providing remote computing service to the public shall not knowingly divulge to any person or entity the contents

of any communication which is carried or maintained on that service on behalf of, and received by means of electronic transmission from (or created by means of computer processing of communications received by means of electronic transmission from), a subscriber or customer of such service." 18 U.S.C. § 2702(a)(2)(A).

52. The SCA defines "remote computing service" as "the provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2).

53. An "electronic communications system" is defined by the SCA as "any wire, radio, electromagnetic, photooptical or photoelectronic facilities for the transmission of wire or electronic communications, and any computer facilities or related electronic equipment for the electronic storage of such communications." 18 U.S.C. § 2510(14).

54. Through its payment processing equipment, Target provides an "electronic communication service to the public" within the meaning of the SCA because it provides consumers at large with credit card and debit card payment processing capability that enables consumers to send or receive wire or electronic communications concerning their account data to transaction managers, card companies or banks.

55. By failing to take commercially reasonable steps to safeguard sensitive consumer financial data, including data of Plaintiffs and the other members of the Class, Target has knowingly divulged customer credit and debit card account information and PINs that were communicated to financial institutions solely for the customer's payment verification purposes, while in electronic storage in Target's electronic systems due to the security breach of their computer storage systems.

56. Further, upon learning that its servers and computer storage systems had been

intruded upon and information had been obtained and accessed by third-parties, Target failed to safeguard its systems, failed immediately to inform customers or the public of the security breach, and continued knowingly to divulge customers' information to third-parties.

57. As a result of Target's conduct described herein and its violations of the SCA, Plaintiffs and the other members of the Class have suffered injuries as described above.

58. Plaintiffs, on their own behalf and on behalf of the other members of the Class, seek judgment in their favor and against Target awarding them and the other Class members the maximum statutory damages available under 18 U.S.C. § 2707, including punitive damages for willful or intentional violations, and including the cost for three years of credit monitoring and identity theft protection services.

AS AND FOR A SECOND CAUSE OF ACTION
(Negligence)

59. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

60. Target assumed a duty of care deriving from the nature of services provided, the catastrophic consequences of breach of security, and the nature of the relationship between Plaintiffs and Class members with Target. Thus, Target was required it to exercise reasonable care to secure and safeguard Plaintiffs' and members of Class' personal and financial information in accepting Plaintiffs' data in connection with Target's sale of goods to Plaintiffs and Class members, and in storing such information in its computer storage systems.

61. Targets breached its duty of care by failing to provide reasonable security and by failing to protect Plaintiffs' and the other Class members' personal and financial data from being captured, accessed, disseminated, and misused by third parties.

62. Target also breached its duty of care by failing to provide accurate, prompt, and

clear notification to Plaintiffs and members of the Class that their personal and financial data had been compromised by unauthorized third-parties.

63. As a direct and proximate result of Target's failure to exercise reasonable care and use commercially reasonable security measures, Target was the direct and proximate cause of Plaintiffs' and the other Class members' injuries as described above.

64. Plaintiffs and members of the Class have suffered an injury in fact and will continue to suffer harm as a result of Target's negligence.

AS AND FOR A THIRD CAUSE OF ACTION
(Negligence *Per Se*)

65. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

66. Target's violations of the SCA and the other statutory violations as alleged herein (including the New York Deceptive Practices Act (N.Y. Gen. Bus. L. § 349), New York's data breach notification statute (N.Y. Gen. Bus. L. § 899-aa), the Illinois Personal Information Protection Act (815 I.L.C.S. 530/1, *et seq*., and the Illinois Consumer Fraud and Deceptive Business Practices Act, 815 I.L.C.S. 505/1, *et seq.*), constitute negligence *per se* as the violation of specific duties imposed by statute.

67. Plaintiffs and the other members of the Class are the intended beneficiaries of the foregoing statutes designed to prevent fraud and deceptive practices against consumers and to address data theft and security breaches.

68. The harm suffered by Plaintiffs and the other members of the Class are specifically the types of harm the foregoing statutes were designed to prevent and/or to address.

69. Target has violated the foregoing statutes without justification or excuse by, among other things, failing to provide immediate notice to customers concerning the theft of

their personal and financial data.

70. As a direct and proximate cause of Target's violations of the foregoing statutes, Plaintiffs and the other members of the Class have suffered and continue to suffer harm and damages stemming from the data breach of Target's electronic systems.

AS AND FOR A FOURTH CAUSE OF ACTION
(Violation of New York General Business Law § 349)

71. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

72. Upon information and belief, Target willfully or knowingly engaged in deceptive and misleading representations and omissions aimed at deceiving reasonable consumers and the public that Target was taking reasonable steps to secure customers' personal and financial information collected in processing payment transactions in Target's stores.

73. Target led customers to believe that their personal and financial information would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

74. As a direct and proximate cause of Target's conduct as alleged herein, Plaintiffs and the Class have suffered and continue to suffer harm and damages stemming from the data breach of Target's electronic systems.

AS AND FOR A FIFTH CAUSE OF ACTION
(Violation of New York General Business Law § 899-aa)

75. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

76. New York General Business Law § 899-aa requires businesses operating in New York State that maintain computerized data including customer personal and financial

information, such as Target, to notify such customers immediately upon discovering a breach of their systems if customer information was or is reasonably believed to have been accessed or acquired by unauthorized persons.

77. As alleged herein, Target failed to notify its customers (including Plaintiffs and the other Class members) immediately upon the discovery of the data breach in which up to 70 million of its customers' information was stolen. Instead, Target waited four days before providing such notice, in violation of General Business Law § 899-aa.

78. As a direct and proximate cause of Target's conduct as alleged herein, Plaintiffs and the Class have suffered and continue to suffer harm and damages stemming from the data breach of Target's electronic systems.

AS AND FOR A SIXTH CAUSE OF ACTION
(Violation of Illinois Consumer Fraud and
Deceptive Business Practices Act, 815 I.L.C.S 505/1, *et seq.*)

79. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

80. Upon information and belief, Target willfully or knowingly engaged in deceptive and misleading representations and omissions aimed at deceiving reasonable consumers and the public that Target was taking reasonable steps to secure customers' personal and financial information collected in processing payment transactions in Target's stores.

81. Target led customers to believe that their personal and financial information would be held in confidence and would be reasonably secure against invasion, intrusion, and infiltration by unauthorized parties.

82. The Illinois Personal Information Protection Act (815 I.L.C.S. 530/1, *et seq*.) provides that a violation thereof constitutes a violation of the Illinois Consumer Fraud and

Deceptive Business Practices Act.

83. As alleged herein, Target violated the Illinois Personal Information Protection Act through its negligent and improper storage of customer personal and financial information that was stolen during the data breach and through its failure to provide immediate notice to customers following the data breach.

84. As a direct and proximate cause of Target's conduct as alleged herein, Plaintiffs and the Class have suffered and continue to suffer harm and damages stemming from the data breach of Target's electronic systems.

AS AND FOR A SEVENTH CAUSE OF ACTION
(Violation of Illinois Personal Information Protection Act, 815 I.L.C.S 530/1, *et seq.*)

85. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

86. The Illinois Personal Information Protection Act requires businesses operating in Illinois that maintain computerized data including customer personal and financial information, such as Target, to notify such customers immediately upon discovering a breach of their systems if customer information was or is reasonably believed to have been accessed or acquired by unauthorized persons.

87. As alleged herein, Target failed to notify its customers (including Plaintiffs and the other Class members) immediately upon the discovery of the data breach in which up to 70 million of its customers' information was stolen. Instead, Target waited four days before providing such notice, in violation of the Illinois Personal Information Protection Act.

88. A violation of the Illinois Personal Information Protection Act also constitutes an unlawful practice under the Illinois Consumer Fraud and Deceptive Business Practices Act.

89. As a direct and proximate cause of Target's conduct as alleged herein, Plaintiffs

and the Class have suffered and continue to suffer harm and damages stemming from the data breach of Target's electronic systems.

AS AND FOR AN EIGHTH CAUSE OF ACTION
(Breach of Implied Contract)

90. Plaintiffs repeat and reallege each and every one of the foregoing allegations as though fully set forth herein.

91. In providing their personal and financial data, Plaintiffs and the other members of the Class entered into an implied contract with Target whereby Target became obligated reasonably to safeguard Plaintiffs' and the other Class members' sensitive, non-public, information.

92. Under such implied contracts, Target was obligated not only to safeguard customer financial information, but also to provide customers with prompt, adequate notice of any security breach or unauthorized access of said information.

93. Target breached the implied contracts with Plaintiffs and the other members of the Class by failing to take reasonable measures to safeguard their financial data.

94. Target also breached its implied contracts with Plaintiffs and the other Class members by failing to provide prompt, adequate notice of the security breach and unauthorized access of customer financial information.

95. Plaintiffs and the other Class members suffered and will continue to suffer harm including, but not limited to loss of their financial information, loss of money and costs incurred as a result of increased risk of identity theft.

JURY TRIAL DEMAND

96. Plaintiffs and the other Class members demand a trial by jury on all issues and claims subject to the right of a jury trial.

REQUEST FOR RELIEF

WHEREFORE, Plaintiffs request the entry of judgment in their favor and against Target: (i) certifying this action as a class action; (ii) appointing Plaintiffs as Lead Plaintiffs; (iii) appointing Plaintiffs' counsel as Class Counsel; (iv) award compensatory damages in an amount to be determined at trial; (v) awarding punitive damages in an amount to be determined at trial; (vi) awarding credit monitoring services for Plaintiffs and the Class members for a period of at least three years to be paid for by Target; (vii) interest, costs, expenses, and attorneys' fees incurred by Plaintiffs and the Class; and (viii) such other and further relief as the Court deems just and proper.

Dated: New York, New York
January 15, 2014

Respectfully submitted

NAPOLI BERN RIPKA SHKOLNIK, LLP

By: /s/ Brian H. Brick
Hunter J. Shkolnik, Esq.
Brian H. Brick, Esq.

350 Fifth Avenue, Suite 7413
New York, New York 10118
(212) 267-3700 (Phone)
(212) 587-0031 (Fax)
Attorneys for Plaintiff